Communiqués et discours

Discours

DES TECHNOLOGIES DE SURVEILLANCE SOUS SURVEILLANCE
par Jennifer Stoddart, Présidente Commission d'accès à l'information

Ce texte a été rédigé en collaboration avec Me Andr é Ouimet,
Secrétaire et Directeur du service juridique à la Commission d'accès à l'information

Septembre 2001

1. La biométrie: fascination et inquiétude

Souvent, lorsque certaines espèces sont menacées d'extinction, des biologistes en capturent des spécimens, leur enfilent une bague, en général sur l'oreille et les remettent dans la nature. Cette technologie permet d'étudier le comportement des survivants, de vérifier s'ils se reproduisent, de contrôler l'espèce, au besoin et, si possible, d'en assurer la pérennité.

Je ne sais pourquoi mais ce sont ces images d'animaux traqués et identifiés qui me sont venus à l'esprit la première fois que j'ai entendu parler de biométrie. Allait-on maintenant traquer l'être humain et le reconnaître entre tous et toutes selon un signalement anthropométrique?

La science et mes lectures allaient me démontrer d'abord les limites de la technologie (la biométrie a ses limites) et que l'outil n'était certainement pas destiné à suivre à la trace des individus. J'ai appris, par exemple, qu'en comparaison aux systèmes d'authentification qui utilisent un objet ou un mot de passe, qui offrent une réponse stable (oui ou non), la biométrie donne des résultats plus fluctuants en terme de pourcentage. Les réponses sont variables, le taux de 100% n'étant jamais atteint[(1)].

Néanmoins, le développement de ces technologies inquiète et fascine tout à la fois. On y subodore la société que George Orwell a longuement décrite dans son livre " 1984 ". Or, on ne peut que supposer un développement toujours plus grand des technologies encore en émergence. L'histoire est riche en leçons à cet égard. Trois exemples en particulier me viennent en tête:

> *" Je pense qu'il y a peut-être un marché mondial pour cinq ordinateurs ", " je ne vois pas pourquoi quelqu'un voudrait avoir un ordinateur à la maison ".*
>
> *" Quand l'exposition de Paris se terminera, la lumière électrique s'éteindra en même temps et nous n'en entendrons plus parler ".*

Ces propos ne furent pas tenus par de quelconques techno-résistants. Dans le premier cas, ils furent tenus par le président d'IBM en 1943; par le président de Digital Equipment Corp. en 1977 dans le deuxième cas et la dernière remarque revient à un professeur de Oxford University en 1878.

Beaucoup d'autres " prophètes " ont annoncé eux aussi la mort prochaine de certaines technologies. Pourtant l'histoire nous enseigne que lorsqu'une technologie est commercialisée, elle est en général vouée à de grands succès commerciaux.

Est-ce dû à cette fascination qu'exerce la technologie ou à une insécurité grandissante, toujours est-il qu'un sociologue pourrait expliquer mieux que moi ce qui amène le développement de ces technologies de surveillance au moment même où dans plusieurs pays la criminalité est à la baisse. Car la technologie est relativement jeune. Certes on utilise depuis longtemps les empreintes digitales à des fins d'identification. Cependant, tel qu'on l'entend aujourd'hui, ce n'est que tout récemment qu'on a vu apparaître la description de la biométrie[2].

Or, comme c'est souvent le cas dans nos sociétés modernes, la biométrie a été, malgré son jeune âge, étudiée, analysée, critiquée. À lui seul, le site internet du Electronic Privacy information Center (EPIC) recense des dizaines d'articles de journaux, épingle plusieurs textes de fond et réfère à plusieurs entreprises spécialisées.

En parallèle, les publications et les séminaires sur le sujet se multiplient au même rythme que se développe la biométrie.

Sans l'ombre d'un doute, sans être grand devin sans flagornerie, il faut croire que la biométrie telle qu'on la conçoit aujourd'hui est là pour rester.

Est-ce là objet d'inquiétude? oui et non! Sans doute associera-t-on à la biométrie de grande vertu. Quant à moi, ce qui inquiète, c'est l'accessibilité accrue à un arsenal technologique sophistiqué par des entreprises, des organismes gouvernementaux ou même voire de simples citoyens[3].

L'anecdote qui suit est révélatrice à cet égard. Au centre-ville de Toronto, un magasin vend une panoplie d'équipements destinés à la surveillance en vue, notamment, d'assurer la sécurité de son propriétaire. Récemment, une dame a acheté une mini-caméra sans fil capable de transmettre des images à une distance d'environ 90 mètres. Le but de l'achat: trouver qui brisait les fleurs de son jardin.

La miniaturisation de tels appareils de surveillance n'a d'égal que la baisse des prix qui l'accompagne. Une mini-caméra qui se vendait environ $800 US il y a dix ans en vaut maintenant $90 US. " At such a price, virtually anybody can get their hands on the technology " s'est exclamé un marchand d'Ottawa. Vous doutez d'un tel scénario, écoutez alors celui qui suit:

> *" Vous êtes dans le hall d'un hôtel fréquenté par des gens d'affaires, dans une grande ville quelque part dans le monde. Vous vous approchez d'une personne qui vous salue de la main. Une caméra miniature logée dans le bouton de votre veston saisit l'image de son visage.*
>
> *Grâce au protocole de communications sans fil Bluetooth, la caméra transmet l'image à votre ordinateur de poche, qui la compare à l'aide*

d'un programme de reconnaissance de visages avec l'image d'autres personnes que vous avez rencontrées.

Si vous en doutiez, vous avez déjà rencontré cette personne il y a six mois dans une foire commerciale. L'ordinateur vous glisse à travers votre écouteur, que vous portez de toute façon car il est relié à votre téléphone mobile, le nom et la fonction de votre interlocuteur, pendant que vous lui serrez la main.

La conversation s'engage. Un autre programme de votre ordinateur de poche analyse la voix de votre vis-à-vis pour y détecter des intonations typiques du mensonge ou de la nervosité.

Bienvenue dans le monde des rencontres d'affaires en 2007.

En tout cas, c'est l'une des visions dans la boule de cristal de Nick Jones, l'un des gourous de la firme de consultants Gartner Group "[4].

Aujourd'hui, j'aimerais partager avec vous quelques réflexions qu'inspire cette " démocratisation " des technologies de surveillance et surtout du fait que si, comme organisme de contrôle, nous pouvons assurer un encadrement légal dans les secteurs publics et privés, qu'en est-il lorsque ce sont nos concitoyens qui les utilisent? Est-il nécessaire de surveiller l'utilisation de ces technologies par les citoyens? Si oui, qui le fera? En est-on rendu à vivre dans un monde où chacun surveille l'autre; les parents surveillent la gardienne, les chauffeurs d'autobus scolaire, les voisins se surveillent mutuellement ! Le simple rappel de ces faits évoquent des années sombres de l'histoire de l'humanité.

2. Les technologies de l'information: une initiative originale au Québec

C'est devenu presqu'un cliché: les technologies de l'information évoluent à un rythme effarant.

À titre de nouvelle présidente d'un organisme voué à la protection des données, je comprends que je n'ai pas à vous rappeler les multiples initiatives prises par différents états pour assurer aux données personnelles toute la protection requise que ce soit dans le vaste secteur public ou encore dans les entreprises privées.

De même, plusieurs d'entre vous êtes déjà intervenus pour rappeler aux uns et aux autres leurs obligations lors de l'utilisation d'outils de surveillance, caméra, biométrie ou autres[5]. L'an dernier, à pareille date, le professeur Vitalis avait présenté un texte d'un grand intérêt sur la vidéosurveillance[6].

Mes lectures de vos documents ou d'autres textes, à l'instar de ceux publiés par la Commission d'accès à l'information du Québec, révèlent qu'outre les spécificités propres à certaines technologies, l'angle d'analyse repose sur ce qu'il est convenu d'appeler les Fair Information Practises que David Flaherty avait lui-même rappelé dans son livre " *Privacy in a surveillance Society* ". Ces règles portent notamment sur la cueillette, la conservation, la finalité, l'utilisation, la communication des renseignements personnels et leur accès par la personne concernée[7].

J'aimerais partager avec vous une initiative originale prise par l'Assemblée nationale du Québec au regard des technologies de l'information. Internet est maintenant devenu un outil utilisé par de plus en plus d'adeptes dans le monde. Convivial, il assure un accès à des ressources illimitées, permet de converser avec des gens qui partagent nos préoccupations partout dans le monde, de faire connaître nos propres réalisations et même d'acheter des produits. Il nous sensibilise aux nouvelles découvertes. Le monde au bout des doigts!

L'une des grandes difficultés, c'est qu'on ne sait jamais à qui on a affaire. Tout au plus, connaît-on son adresse électronique! Dans certains cas, c'est sans conséquence. Dans d'autres, achats en ligne, transaction avec le gouvernement ou une entreprise, l'enjeu est de taille. Le gouvernement ou l'entreprise doit s'assurer qu'elle fait affaire avec la bonne personne.

Dans cette perspective, l'Assemblée nationale du Québec vient d'adopter la *Loi concernant le cadre juridique des technologies de l'information*[8] qui a pour objet d'assurer notamment la sécurité juridique des communications effectuées au moyen de documents, l'équivalence fonctionnelle des documents et leur valeur juridique, quels qu'en soient les supports, ainsi que l'interchangeabilité de ces derniers. Elle vise également à assurer la concertation en vue d'harmoniser les systèmes, les normes et les standards techniques permettant la communication au moyen de documents technologiques.

Plusieurs originalités caractérisent cette loi. Ainsi, elle reconnaît la possibilité d'utiliser divers modes d'authentification de l'identité d'une personne qui communique au moyen d'un document technologique et, dans ce contexte, elle contient des mesures de protection de la vie privée. De plus, la loi affirme la nécessité et prévoit des moyens de faire le lien entre une personne et le document par lequel elle exprime sa volonté ainsi que le lien du document avec une association, une société ou l'État. À cet égard, la loi contient des dispositions pour baliser la prestation de services de certification et de répertoire et offre à tout prestataire de services de certification, qu'il soit du Québec ou d'ailleurs, de se faire accréditer, en fonction des mêmes critères d'appréciation, par une personne ou un organisme déterminé par le gouvernement.

Au chapitre des droits fondamentaux, cette loi n'écarte ni les lois qui assurent la protection des données personnelles pas plus qu'elle n'enlève de juridiction à la Commission d'accès à l'information. Bien au contraire, cette loi prévoit que nul ne peut exiger que l'identité d'une personne soit établie au moyen d'un procédé ou d'un dispositif qui porte atteinte à son intégrité physique. À moins que la loi le prévoie expressément en vue de protéger la santé des personnes ou la sécurité publique, nul ne peut exiger qu'une personne soit liée à un dispositif qui permet de savoir où elle se trouve.

De même, la loi précise que nul ne peut exiger, sans le consentement exprès de la personne, que la vérification ou la confirmation de son identité soit faite au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques. L'identité de la personne ne peut alors être établie qu'en faisant appel au minimum de caractéristiques ou de mesures permettant de la relier à l'action qu'elle pose et que parmi celles qui ne peuvent être saisies sans qu'elle en ait connaissance.

En outre, cette nouvelle loi se fait forte de garantir aux citoyens que tout autre renseignement la concernant et qui pourrait être découvert à partir des caractéristiques ou mesures saisies ne peut servir à fonder une décision à son égard ni être utilisé à quelque autre fin que ce soit. Un tel renseignement ne peut être communiqué qu'à la personne concernée et seulement à sa demande.

Ces caractéristiques ou mesures ainsi que toute note les concernant doivent être détruites lorsque l'objet qui fonde la vérification ou la confirmation d'identité est accompli ou lorsque le motif qui la justifie n'existe plus.

Le législateur a aussi prévu que la création d'une banque de caractéristiques ou de mesures biométriques doit être préalablement divulguée à la Commission d'accès à l'information. De même, doit être divulguée l'existence d'une telle banque qu'elle soit ou ne soit pas en service.

La Commission peut rendre toute ordonnance concernant de telles banques afin d'en déterminer la confection, l'utilisation, la consultation, la communication et la conservation y compris l'archivage ou la destruction des mesures ou caractéristiques prises pour établir l'identité d'une personne.

La Commission peut aussi suspendre ou interdire la mise en service d'une telle banque ou en ordonner la destruction, si celle-ci ne respecte pas ses ordonnances ou si elle porte autrement atteinte au respect de la vie privée.

Il y a lieu de saluer l'initiative à laquelle la Commission a participé par ses experts et par sa contribution lors de l'étude du projet de loi devant une commission parlementaire de l'Assemblée nationale. Adoptée en juin dernier, la Commission que je préside n'a pas encore précisé la façon dont ce nouveau mandat sera exercé. Nous pensons émettre éventuellement des lignes directrices à partir de cas concrets. J'ai pris connaissance d'un certain nombre de textes que des commissaires ont déjà produits sur la biométrie. La CNIL, notre hôte cette année, a notamment publié un texte d'une grande qualité reprise dans les pages de son rapport d'activités. Néanmoins, je compte profiter de notre rencontre pour prendre conseil. À l'avance, je vous remercie pour toute contribution. En échange, je vous promets que l'an prochain, je serai en mesure de vous faire un premier bilan de notre expérience.

3. Concilier technologie et droits de la personne

S'il me faut saluer l'adoption de la *Loi concernant le cadre juridique des technologies*, il me faut aussi souligner l'émergence de nouvelles problématiques pour lesquelles je n'ai encore trouvé aucune réponse. Je l'ai dit d'entrée de jeu, les technologies de surveillance ne sont plus l'apanage des corps policiers, des grandes sociétés, des pouvoirs publics: Parents, petit propriétaire d'un immeuble, garderie d'enfants, les moyens de surveillance électroniques et sophistiqués sont désormais à la portée de tous. Si ce n'est pas déjà le cas, ils le seront!

Ce que nous appelons téléphone cellulaire et qui décrit ce qu'outre-atlantique, vous appelez " portable " justifierait à lui seul une réflexion. Localiser un individu à l'aide de cet appareil est évident. Des personnes perdues dans des régions éloignées sont localisées grâce à leur " portable ". Il existe évidemment des modes de localisation plus sophistiquées et maintenant facilement accessibles. Bracelets, appareils GPS, transpondeurs n'en constituent que quelques exemples.

Devant le phénomène de surveillance qui inévitablement suscitera de nouveaux débats, soulèvera de nouveaux enjeux, quelles sont les solutions qu'apportent nos lois dont les objectifs avoués sont de protéger nos renseignements personnels?

Dans la mesure où des individus eux aussi pourront de plus en plus facilement recueillir, traiter, conserver et même communiquer des données personnelles, l'état

doit-il intervenir? Les organismes auxquels nous appartenons devraient-ils, d'ores et déjà, sonner l'alarme? Le législateur est souvent intervenu pour protéger les données personnelles détenues par le secteur privé parce que souvent, nous l'avons convaincu que, peu importe le détenteur, organismes publics ou entreprises, elles méritaient la même protection. Cette logique qui a présidé à l'adoption des lois qui protègent les données personnelles détenues dans le secteur privé, ne devrait-elle pas justifier une intervention législative pour assurer des limites à une société de surveillance mutuelle. La situation m'apparaît déjà suffisamment préoccupante pour qu'on s'y arrête. Évidemment, il est possible de transposer les mécanismes de protection offerts aux renseignements détenus par l'État ou l'entreprise. Toutefois, la réalité particulière de la détention de renseignements personnels par des individus commande fort probablement une approche originale. À problèmes nouveaux, solutions nouvelles!

Encore là, je m'en remets à l'expérience que nous cumulons ensemble pour réfléchir sur la problématique et après réflexion, je vous invite à en discuter. Les droits de la personne ne sont pas en cause uniquement lorsque c'est l'État ou l'entreprise qui recueillent des données.

1.° Voir notamment le 21e rapport d'activités 2000, Commission nationale de l'informatique et des libertés, p. 101 et ss.

2.° Dans son livre " The transparent society ", David Brin, en 1998 parle, avec un certain cynisme, il est vrai, d'un " new field of biometric identification ".

3.° Micro-Spying marker grows, The Gazette, September 6, 2001, p. A-12.

4.° Les bidules de Big Brother, La Presse, 16 mars 2001, p. D-3.

5.° Voir par exemple les textes publiés par le bureau de notre collègue Ann Cavoukian sur la reconnaissance biométrique dans les casinos et les aéroports de l'Ontario.

6.° Vitalis, André, Towards an electronic Citizenship, 22e Conférence internationale des Commissaires à la protection des données, Venise, Septembre 2000.

7.° Flaherty, David H., Protecting privacy in surveillance society, The University of North Caroline Press, 1989, p. 380.

8.° Lois du Québec, 2001, chapitre 32.

Politique de confidentialité | Copyrights